In the Office Action, Claim 3 was objected to because the claim defines the object key as being dynamic and further defines that the object key changes with each data block encrypted. The Examiner contends that such language is redundant. Applicant respectfully traverses the Examiner's objection and notes that although the object key is dynamic, the further limitation that the object key changes with each data block encrypted is not redundant. Reconsideration of this rejection is respectfully requested.

In the Office Action, Claim 15 was objected to as being dependent upon Claim 17. By this amendment, Claim 15 has been amended to depend upon Claim 5. Accordingly, reconsideration of the objection of Claim 15 is respectfully solicited.

In the Office Action, each of Claims 1, 9, 12, 17-20 and 22 were rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 5,724,428 to Rivest in view of U.S. Patent No. 5,369,702 to Shanton. Furthermore, each of Claims 3-8, 11, 13, 14, 16, 29, 31-32 and 34 were rejected as being unpatentable over the Rivest reference in view of the Shanton reference and further in view of selected pages from the Handbook of Applied Cryptography, authored by Menezes, et al. Lastly, each of Claims 10-15, 21, 23-24 and 30 were rejected as being unpatentable over the Rivest reference in view of the Shanton reference and further in view of well known art.

The present invention is directed to an iterative block cipher encryption method which utilizes a dynamic key schedule to create a one to many mapping of plaintext and ciphertext utilizing a specific key. More specifically, the dynamic key schedule includes an object key comprising data and methods that operate on the data. The object key is created by the user and the method that modifies the object key is based on seeding from a random session object key. The key modification is performed for each input plaintext data block so that each data block is encrypted with a different key. Accordingly, this one to many mapping of plaintext and ciphertext utilizing the dynamic object key as defined in the specification and claims provides a block cipher encryption method which encrypts each plaintext data block utilizing a different key schedule to produce ciphertext that is virtually immune to cryptanalytic attack designed to work with static key schedules.

Conventional iterative block ciphers (DES,IDEA,RC5,RC6, etc.) are basically comprised of monoalphabetic substitution ciphers with block length characters. Under a specific key, whenever the same plaintext block goes into the cipher, the same ciphertext block is generated by the encryption process. The present iterative block cipher encryption method teaches away from the use of static key schedules by providing an object key which changes with each data block being encrypted.

Referring now to the independent claims, independent Claim 1 defines a method for encrypting data comprising the steps of creating an object key comprising data and methods that operate on the data and encrypting input plaintext data utilizing the object key in conjunction with an encryption process. Independent Claim 30 further provides that the dynamic object key changes with each block of input data and that each object key is associated with a different key schedule to encrypt/decrypt the input plaintext /output ciphertext message. Lastly, independent Claim 25 is directed to a computer implemented method for authenticating ciphertext including generating a digital signature of a user using the ciphertext as input into a keyed one-way hash function and appending the digital signature to the input ciphertext. Applicant respectfully urges, as will be discussed in further detail below, that none of the cited references of record teach or suggest the invention as defined in independent Claims 1, 25 and 30.

U.S. Patent No. 5,724,428 to Rivest discloses an encryption and decryption method using data-dependent rotations. The amount of rotations depends upon the data being encrypted and intermediate encryption results. The basic encryption algorithm is a block cipher encryption method. It appears that the Rivest reference was cited merely as disclosing a block cipher encryption method although it is evident that the invention disclosed in the Rivest reference is clearly different from the encryption method disclosed in the present application. Rivest fails to teach or suggest the use of the claimed dynamic object key to create ciphertext. Accordingly, it is believed that no further comment regarding the Rivest reference is necessary at this time.

U.S. Patent No. 5,369,702 to Shanton discloses a system providing multilevel multimedia security in a data network by creating an object-oriented encryption system. Once an object is created, it can be encrypted, labeled and embedded in other objects. An object as defined in the specification can include a bit of information, a byte of information, sound clips, video clips, graphic images, text, charts, tables, forms, controls, variables, executable files, video files, binary files, etc. (see column 3, lines 41-57). The multilevel security of the invention is achieved because encrypted objects may be nested within another object which are also encrypted, possibly within another object resulting in multiple layers of encryption. The system is designed to allow only those users with access keys to retrieve the encrypted objects.

A

The definition of an object as set forth in the Shanton reference is very different from the dynamic object key which comprises data and methods that operate on the data in a block cipher encryption process as described and claimed in the present application. More specifically, the object key of the present invention is specifically used as a device to encrypt input plaintext data to create ciphertext. To the contrary, Shanton discloses that the objects may be encrypted and embedded in other objects; however, the objects are not in of themselves a part of the encryption process. Accordingly, a combination of the Rivest reference and the Shanton reference does not teach or suggest the claimed encryption method using a object key comprising data and methods that operate on the data to create ciphertext. Furthermore, there is no teaching or suggestion in the Shanton reference to use his object-oriented multilevel security system in a block cipher encryption method such as that disclosed in the present invention and the Rivest reference. Accordingly, it would not be obvious to one of ordinary skill in the art to combine the teachings of the Shanton reference with those of the Rivest reference, even though they are in the same general field of encryption. Reconsideration of the rejections to each of the claims in view of the Rivest and Shanton references is respectfully solicited.

In the Office Action, the Examiner also relies on the Handbook of Applied Cryptogtraphy in the rejection of several of the dependent claims. For example, the Examiner comments that the Menezes book teaches a computer implemented method wherein the object key is dynamic for each encrypted data block reciting to pages 490-491. However, the book references a "dynamic key establishment" for a session key and that the session key should be dynamic. The reference further teaches that the session key can change for each session. However, a session is not defined and most probably consists of many data blocks. The reference does not teach or suggest the use of a computer implemented method wherein an iterative block cipher encryption process utilizes a dynamic object key based on a dynamic key schedule which changes for each block of data being encrypted.

Furthermore, the reference to pages 20-21 and 170 of the Menezes reference teaches the methods of extreme ciphers and pseudorandom bit generators. Extreme ciphers and iterative block ciphers are substantially different in their function, use and design. The present invention specifically defines an iterative block cipher encryption method. The Menezes references fails to teach or suggest an iterative block cipher encryption method utilizing a dynamic object key and a dynamic key schedule for each block of data to be encrypted.

With respect to pages 255-256, the Menezes reference describes the key schedule of DES. The key schedule for DES is static for each block of data. In DES, under a specific key, the same ciphertext will be produced if the same plaintext enters the cipher. This is completely contrary to the claimed present invention in which the dynamic object key and dynamic key schedule changes for each block of plaintext such that the same plaintext does not create the same ciphertext using the encryption method of the present invention. Furthermore, with reference to page 252, the Menezes book describes an S box in the DES algorithm. As previously noted, these particular S boxes are fixed (static) and are used once for every six bits in each round. Contrawise, the present invention utilizes a keyed substitution repetition amount for each round for each ciphertext byte, i.e., a ciphertext byte is repeatedly sent through a substitution box for each round and the repetition amount is key dependent. Additionally, the S boxes of the present invention are dynamic not static. These distinct differences further highlight the teaching away of known encryption methods from that of the present invention.

Accordingly, reconsideration of the rejections involving the Menezes book are respectfully solicited.

In view of the foregoing amendments and remarks, favorable consideration of Claims 1-35 are respectfully solicited. If the Examiner believes that a telephone interview would expedite allowance of this application, she is respectfully requested to contact Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

Glenn T. Henneberger
Registration No.: 36,074
Attorney for Applicant

HOFFMANN & BARON, LLP
6900 Jericho Turnpike
Syosset, New York 11791
(516) 822-3550

GTH/mpf

101967_1.DOC